FIPS PUB 113

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

1985 MAY 30

U.S. DEPARTMENT OF COMMERCE/National Bureau of Standards

COMPUTER DATA AUTHENTICATION

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, Secretary
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of Government efforts in the development of guidelines and standards in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Institute for Computer Sciences and Technology, National Bureau of Standards, Gaithersburg, MD 20899.

James H. Burrows, Director Institute for Computer Sciences and Technology

Abstract

This publication specifies a standard to be used by Federal organizations which require that the integrity of computer data be cryptographically authenticated. In addition, it may be used by any organization whenever cryptographic authentication is desired. Cryptographic authentication of data during transmission between electronic components or while in storage is necessary to maintain the integrity of the information represented by the data. The standard specifies a cryptographic authentication algorithm for use in ADP systems and networks. The authentication algorithm makes use of the Data Encryption Standard (DES) cryptographic algorithm as defined in Federal Information Processing Standard 46 (FIPS PUB 46).

Key words: authentication; cryptography; data authentication algorithm; Data Encryption Standard (DES); data integrity; Federal Information Processing Standard (FIPS).

Nat. Bur. Stand. (U.S.) Fed. Info. Process. Stand. Pub. (FIPS PUB) 113,6 pages (1985) CODEN:FIPPAT

For sale by the National Technical Information Service, U.S.

Department of Commerce, Springfield, VA 22161.

FIPS PUB 113

Federal Information
Processing Standards Publication 113

1985 May 30

Announcing the Standard for
COMPUTER DATA AUTHENTICATION

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to section 111 (f) (2) of the Federal Property and Administrative Services Act of 1949, as amended. Public Law 89-306 (79 Stat. 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of the Title 15 Code of Federal Regulations (CFR).

Name of Standard: Standard on Computer Data Authentication (FIPS PUB 113).

Category of Standard: ADP Operations, Computer Security.

Explanation: This standard specifies a Data Authentication Algorithm (DAA) which may be used to detect unauthorized modifications, both intentional and accidental, to data, The standard is based on the algorithm

specified in the Data Encryption Standard (DES) Federal Information Processing Standards Publication (FIPS PUB) 46, and is compatible with both the Department of the Treasury's Electronic Funds and Security Transfer Policy and the American National Standards Institute (ANSI) Standard for Financial Institution Message Authentication (see cross index). The Message Authentication Code (MAC) as specified in ANSI X9.9 is computed in the same manner as the Data Authentication Code (DAC) specified in this standard. Similarly, the Data Identifier (DID) specified in this standard is sometimes referred to as a Message Identifier (MID) in standards related to message communications. The example given in Appendix 2 may be used when validating implementations of this standard.

Approving Authority: Secretary of Commerce.

Maintenance Agency: U.S. Department of Commerce, National Bureau of Standards, Institute for Computer Sciences and Technology.

Cross Index:

ANSI X9.9-1982, American National Standard for Financial Institution Message Authentication, April 13, 1982.

ANSI X9. 17-1985, American National Standard for Financial Institution Key Management (wholesale), April 4, 1985.
Department of the Treasury Directives Manual, Electronic Funds and Securities Transfer Policy, Chapter TD 81, Section 80, August 16, 1984.

FIPS PUB 1-2, Code for Information Interchange, Its Representations, Subsets, and Extensions November 14, 1984.
FIPS PUB 46, Data Encryption Standard, January 15, 1977.

FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard April 1, 1981. FIPS PUB 81, DES Modes of Operation. December 2, 1980.

Federal Standard 1026, Telecommunications' Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical and Data Link Layers of Data Communications, August 3, 1983.

Federal Standard 1027, Telecommunications' General Security Requirements for Equipment Using the Data Encryption Standard. April 14, 1982.

FIPS PUB 113

Applicability: This standard shall be used by Federal organizations whenever the person responsible for the security of any computer system or data determines that cryptographic authentication is needed for the detection of intentional modifications of data, unless the data is classified according to the National Security Act of 1947, as amended, or the Atomic' Energy Act of 1954, as amended. Equipments approved for the cryptographic authentication of classified data may be used in lieu of equipments meeting this standard. In all cases, the authorized agency official shall determine that any alternative cryptographic authentication system performs at least as well as those specified in this standard. Use of this standard is also encouraged in private sector applications of cryptographic authentication for data integrity.

Implementation: The DAA may be implemented in hardware, firmware,

software, or any combination thereof. Implementation Schedule: This

standard becomes effective November 30, 1985.

Export Control: Cryptographic devices and technical data regarding them are subject to Federal government export controls either as specified in Title 22, Code of Federal Regulations, Parts !21 through 128, or in Title 15, Code of~Federal Regulations, Parts 368 through 399. as

applicable. Any exports of cryptographic devices implementing this standard and technical data regarding them must comply with these Federal regulations.

Patents: Cryptographic equipment implementing this standard may be covered by U.S. and foreign patents.

Specifications: Federal Information Processing Standard 113 (FIPS 113), Computer Data Authentication (affixed).

Waivers: Heads of agencies may request that the requirements of this standard be waived in instances where it can be clearly demonstrated that there are appreciable performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the requested waiver. Such waiver requests will be reviewed by and are subject to the approval of the Secretary of Commerce. The waiver request must specify anticipated performance and cost advantages in the justification for the waiver.

Forty-five days should be allowed for review and response by the Secretary of Commerce. Waiver requests shall be submitted to the Secretary of Commerce, Washington, DC 20230, and labeled as a Request for a Waiver to Federal Information Processing Standard Publication 113. No agency shall take any action to deviate from the standard prior to the receipt of a waiver approval from the Secretary of Commerce.

Where to Obtain Copies: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 113 (FIPSPUB113), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, credit card, or deposit account.

Federal Information
Processing Standards Publication 113
1985 May 30

Specifications for COMPUTER DATA AUTHENTICATION

1. INTRODUCTION

In automated data processing systems it is often not possible for humans to scan data to determine if it has been modified. Examination may be too time consuming for the vast quantities of

data involved in modern data processing applications, or the data may have insufficient redundancy for error detection. Even if human scanning were possible, the data could have been modified in such a manner that it would be very difficult for the human to detect the modification. For example, "do" may have been changed to "do not" or $1,000 may have been changed to $3 ,000. Without additional information the human scanner could easily accept the altered data as being authentic. These threats may still exist even when data encryption is used. It is therefore desirable to have an automated means of detecting both intentional and unintentional modifications to data. Ordinary error detecting codes are not adequate because, if the algorithm for generating the code is known, an adversary could generate the correct code after modifying the data. Intentional modification is undetectable with such codes. However, a cryptographic Data Authentication Algorithm (DAA) can protect against both accidental and intentional, but unauthorized, data modification.

2. THE DAA AUTHENTICATION PROCESS

A Data Authentication Code (DAC) is generated by applying the DAA to data as described in the following section. The DAC, which is a mathematical function of both the data and a cryptographic key, may then be stored, or transmitted, with the dab When the integrity of the data is to be verified, the DAC is generated on the current data and compared with the previously generated DAC. If the two values are equal, the integrity (i.e., authenticity) of the data is verified.

The DAA detects data modifications which occur between the initial generation of the DAC and the validation of the received DAC. It does not detect errors which occur before the DAC is originally generated.

3. GENERATION OF THE DAC

The Data Authentication Algorithm (DAA) makes use of the Data Encryption Standard (DES) cryptographic algorithm specified in FIPS PUB 46. The DES algorithm transforms (or encrypts) 64-bit input vectors to 64-bit output vectors using a cryptographic key. Let D be any 64-bit input vector and assume a key has been selected. The 64-bit vector, O, which is the output of the DES algorithm when DES is applied to D, using the enciphering operation, is represented as follows.

$$O = e(D)$$

The data (e.g., record, file, message, or program) to be authenticated is grouped into contiguous -bit
blocks: D 1, D2,.... Dn. If the number of data bits is not a multiple
of 64, then the final input block will be

a partial block of data, left justified. with zeroes appended to form a full 64-bit block. The calculation of the DAC is given by the following equations where G represents the Exclusive-OR of two vectors.

$$01 = e(D1)$$

$$02 = e(D2\ C01 \oplus 6)$$

$$03 = e(D3 \oplus 02)$$

$$On = e(Dn \oplus 0n\text{-}1)$$

The DAC is selected from On. Devices which Implement the DAA shall be capable of selecting the leftmost M bits of On as the DAC, where 16 < M < 64 and M is a multiple of 8. A block diagram of the DAC generation is given in Appendix 1 and an example is given in Appendix 2. The Cipher Block Chaining Mode (CBC) with Initialization Vector (IV) = 0 and the 64-bit Cipher Feedback Mode with IV = D1 and data equal to D2, D3, ..., Dn (see FIPS PUB 81) both yield the required DAC calculation.

4. THE AUTHENTICATION OF ASCII CHARACTERS

When 7-bit ASCII (American Standard Code for Information Interchange) coded data is to be authenticated by the DAA, each character processed by the authentication algorithm shall be represented as an 8-bit byte (O, b_7 b_1) where (b_7, b_6 ..., b_1) are defined by FIPS PUB 1-2, Code for Information Interchange. Its Representations, Subsets, and Extensions Thus, a message may have its parity changed without altering its DAC.

5. DELETION AND INSERTION

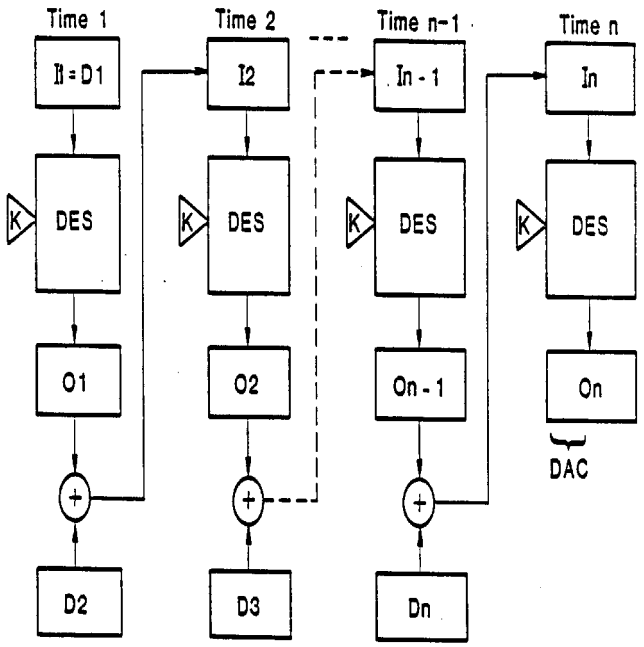
When detection of either the unauthorized deletion or the insertion of an entire authenticated data set is required, a Data Identifier (DID) must be used as part of the authenticated data The DID is a sequence number whose value can be checked whenever the data is authenticated. A gap in the DIDs indicates deletion, while a repeated DID indicates insertion.

6. CRYPTOGRAPHIC KEY SECURITY

The integrity provided by the DAA is based on the fact that it is infeasible to generate a DAC without knowing the cryptographic key. An adversary without knowledge of the key will not be able to modify data and then generate an authentic DAC on the modified data. It is therefore crucial that keys be protected so that their secrecy is preserved- Key management, involving key generation, key distribution, key storage, and key destruction, must be provided. Information pertaining to key management may be found in the American National Standard for Financial Institution Key Management (wholesale), ANSI X9. 17-1985.

APPENDIX 1

BLOCK DIAGRAM OF ThE DAA



D = Data Block
I = Input Block
O = Output Block
DES = Data Encryption Standard
K = DES Key
⊕ = Exclusive-OR

APPENDIX 2

AN EXAMPLE OF THE DAA

Cryptographic Key = 0123456789abcdef

The text is the ASCII code for "7654321 Now is the time for ". These 7-bit characters are written in hexadecimal notation ($0,b_7,b_6,...,b_1$).

Text =
3736353433323120e6f772068732074686520746965206666f7220

TIME	PLAIN TEXT	DES INPUT BLOCK	DES OUTPUT BLOCK
1	3736353433323120	3736353433323120	21fb193693a16c28
2	4e6f772069732074	6f946e16fad24c5c	6c463f0cb7167a6f
3	686520746965206	04231f78de7b1f4f	956ee891e889d91e
4	666f722000000000	f3019ab1e889d91e	f1d30f6849312ca4

A 32-bit DAC = f1d30f68 is selected.